State of Indiana Policy and Standards

Change Management

Standard ID
IOT-CS-ARC-002

Published Date
10/3/2016

Effective Date
1/30/2017

Last Updated
11/15/2016

Next Review Date
11/15/2017

Policy
09.0 Information Protection Processes and Procedures (PR.IP)

09.3 PR.IP-3

09.3.1 Change Management

Purpose
Control changes to service assets and configuration items across the whole service lifecycle, providing a structured, repeatable process that enables necessary changes, while causing minimal disruption to IT services.

Scope
IOT Supported Entities

Statement
The management of any installation or alteration which adds to, deletes from, or modifies any production environment that the Indiana Office of Technology manages is subject to the requirements of this standard, including, but not limited to:

- Application Changes
- Hardware Changes
- Visual Changes
- System or Software Changes
- Firewall Changes
- Network changes impacting many users and/or multiple agencies
- Environmental Changes
- Documentation Changes
- Shared Environments (Production and Non-Production)
- Services and Tools in support of production systems, procedures or environmental facilities

Change Requestor

The individual who will be implementing the change shall be the person who submits the change request. IOT administrator or IOT liaison shall request on the behalf of the agency. Agency must have all production released code submitted through IOT Change

Management Request (CMR).

Change Advisory Board (CAB)

A team of people made up of IOT Managers, Executives and subject matter experts. Additional members will be included depending on the change being analyzed. It is chaired by the IOT Change Administrator and assisted by IOT Change Coordinator. The mission of the Change Advisory Board is to perform the following for all changes introduced into the production environment:

-Plan, approve and monitor

-Review post mortem Emergency and Failed CMRs

-Review the previous week's 24 hr. daily system and network change reports

The IOT Change Coordinator is responsible for strategic communication between agencies and IOT departments.

The CAB will meet every Monday to review and approve any changes that will occur within a two week window. Emergency changes will be handled by the IOT Change Administrator and will potentially call an emergency meeting if the change is significant enough. A Thursday implementation meeting will be held to address any approved changes that have the potential of impacting each other. The meeting will consist of the change requestors, IOT Change Coordinator and IOT Change Administrator. It is the change requestor's responsibility to thoroughly review all other potentially conflicting changes *prior* to the Thursday meeting and have concerns ready for discussion.

Change Request Types

Emergency Change – are those changes that are vital to ensure that its committed service levels are maintained.
- Approved by:
  - Manager of requesting user
  - IOT Change Administrator or emergency CAB meeting
- All Emergency Changes must be post reviewed by CAB

Standard Change – Preauthorized and reoccurring change that is relatively common and follows a procedure or work instruction (Ex..Windows security updates). Reviewed only by IOT Change Administrator.

Normal Change - Changes that require full Change Management review. They are reviewed and approved or rejected by CAB (**DEFAULT**).

All requests that are unsuccessful or any unexpected results WILL be post reviewed by the CAB. The requestor will complete a failed request form prior to the next Monday CAB meeting.

Rating CMR's

CMR's will be rated by classifying the impact and risk involved in the execution of the CMR. Impact and risk will be classified based upon the criteria below and once classified there values will be meshed to give the overall rating for the CMR.

IMPACT classifications – HIGH, MEDIUM, LOW

Determining impact would be an answer to the question:

If your change would be unsuccessful or the process of your change could negatively affect systems, the result would be:

- HIGH –

  Multiple agencies would be affected and/or involves highly used or highly visible systems.

- MEDIUM –

  Single agency would be affected with medium number of users. No highly visible or highly used systems are impacted.

- LOW -

  Single or partial agency with small number of users. No shared environment systems will be affected and not to the

point of interrupting their general work day.

RISK classifications – HIGH, MEDIUM, LOW

The potential risk is associated with the change complexity, dependencies, ability to rollback, and non-production testing

- HIGH –

One or more of the following: Highly complex change, many dependencies, very difficult or impossible to rollback and/or little or no testing of non-production environment

Examples:

- Highly complex change – Upgrading Oracle RAC database. Many steps and a lengthy process
- Very difficult or impossible to rollback - 2003 Domain functionality upgrade to 2008.
- Many dependencies – Java update that many applications dependent on the specific Java version.
- Testing of non-production environment – Most SAN and networking equipment does not have non-production equipment.

- MEDIUM –

One or more of the following: Moderate complexity change, few dependencies, moderate difficulty to rollback with normal testing of non-production environment

- Moderate complexity change – Service pack upgrades to database or operating system
- Moderate difficulty to rollback – Standard rollback that would take about the same amount of time to apply
- Few dependencies – Adding a new VLAN (DHCP scope, network monitoring…etc)
- Normal testing of non-production environment – Database upgrades tested in UAT environment

- LOW -

One or more of the following: Low complexity change, no dependencies, low difficulty or no need to rollback with decisive testing of non-production environment

- Low complexity change – Replacing a raided drive on a physical server
- Low difficulty or no need to rollback – Replacing DIMM in a server
- No dependencies – Replacing a network switch
- Decisive testing of non-production environment – Very extensive testing process that covers all aspects of changing system

Overall CMR Rating - Product of Impact and Risk Ratings

		Risk		
		High	*Medium*	*Low*
Impact	*High*	**MAJOR**	**MAJOR**	**SIGNIFICANT**
	Medium	**MAJOR**	**SIGNIFICANT**	**SIGNIFICANT**
	Low	**SIGNIFICANT**	**SIGNIFICANT**	**MINOR**

CMR Rating Review Period

- MAJOR – There will be a minimum of a four weeks review period for all MAJOR CMR rating
- SIGNIFICANT - There will be a minimum of a two weeks review period for all SIGNIFICANT CMR rating
- MINOR - There will be a minimum of a one week review period for all MINOR CMR rating

Scheduled Change Windows

All changes will be on Sunday 6-10 AM unless valid reasons dictate otherwise. The CAB will determine if it will be necessary to allow request to be done outside of normal window unless the agency has an IOT agreement.

Roles

Information Asset Owners/System Owners

IOT Personnel

Responsibilities

All IOT personnel that have the ability to make changes to the production IT environment shall be required to follow and participate in all outlined required change management meetings and documentation. Agency System Owners must work with appropriate IOT personnel to submit a change management requests on behalf of agency when promoting production code

Management Commitment

Management shall ensure all outlined change management requirements are enforced

Coordination Among Organizational Entities

Agencies shall coordinate with IOT Liaison to submit change management requests on behalf of agency.

Compliance

IOT and Agencies shall review respective system ownership to determine production changes that require to be part of change management

Exceptions

Exceptions will be handled on a case by case basis through the Director of Risk & Compliance, State CISO and the IOT Architecture team.